REMARKS

Claims 1-35 are pending in the present application.

This Amendment is in response to the Non-Final Office Action mailed March 21, 2008. In the Office Action, the Examiner rejected claims 1-32 under 35 U.S.C. §101, and rejected claims 1-35 under 35 U.S.C. §103(a).

Applicant has amended claims 1, 9, 17 to correct minor informalities. Reconsideration in light of the amendments and remarks made herein is respectfully requested.

I. REJECTION UNDER 35 U.S.C. § 101

In the Office Action, the Examiner contends that claims 1-32 are rejected because the claimed invention is directed to non-statutory subject matter. Specifically, the Examiner contends that the claimed invention recites an article of manufacture, a system, and a method while the specification is directed otherwise because the specification is reciting that the claimed invention may be implemented by hardware, software, or any combination. The Examiner then concluded that claims 1-32 are directed to software per se. Applicant respectfully disagrees and believes that the Examiner mis-applied the basic rules of patent examination for the following reasons.

First, the Examiner is not in a position to force the Applicant to claim a certain aspect of the invention according to the Examiner's preference. The specification states that the invention may be implemented by hardware, software, or any combination. Applicant elects to claim the invention in terms of an article of manufacture, a system, and a method. These claims represent aspects of the invention as described in the specification.

Second, the Examiner's conclusion that claims 1-32 are directed to software per se simply based on the statement that the claimed invention may be implemented by hardware, software, or any combination, is clearly erroneous. If

the specification states that the claimed invention may be implemented by hardware, software, or any combination, how could claims 1-32 be directed only to software per se? The word "or" is a conjunctive, indicating that there may be any one of the listed implementation methods. According to the Examiner's argument, if somebody says that "the house may be painted in red, white, or yellow", then the conclusion is that "the house must be painted in white". Clearly, this conclusion defies any sound logic reasoning.

Third, even if claims 1-32 are directed to software, they are not non-statutory. The word "per se" in "computer listings per se" indicates that "descriptions or expressions of the program". They are not patentable because "[t]hey are neither computer components nor statutory processes, as they are not "acts" being performed. Only when the claimed invention taken as a whole is directed to a mere program listing, i.e., to only its description or expression, is it descriptive material per se and hence non-statutory (MPEP 2106.01). The Examiner has not shown that claims 1-32 taken as a whole are directed to mere program listing and/or do not recite acts to be performed. Furthermore, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See Lowry, 32 F.3d at 1583-84, 32 USPQ2d at 1035. MPEP 2106.01 (Emphasis added.)

Fourth, according to Interim Guidelines for Examination of Patent Applications for Subject Matter Eligibility ("Guidelines"), claims 1-32 are statutory under 35 U.S.C. §101. A claimed process is statutory if it is limited to a practical application of the abstract idea or mathematical algorithm in the technological arts. See Alappat, 33 F.3d at 1543, 31 USPQ2d at 1556-57 (quoting Diamond v. Diehr, 450 U.S. at 192, 209 USPQ at 10). See also Alappat 33 F.3d at 1569, 31 USPQ2d at 1578-79 (Newman, J., concurring) ("unpatentability of the principle does not defeat patentability of its practical applications") (citing O'Reilly v. Morse, 56 U.S.

(15 How.) at 114-19). A claim is limited to a practical application when the method, as claimed, produces a concrete, tangible and useful result; i.e., the method recites a step or act of producing something that is concrete, tangible and useful. See AT&T, 172 F.3d at 1358, 50 USPQ2d at 1452. MPEP 2106 IV.B.2.

The Guidelines states: To satisfy section 101 requirements, the claim must be for a practical application of the §101 judicial exception, which can be identified in various ways: (1) The claimed invention "transforms" an article or physical object to a different state or thing; (2) The claimed invention otherwise produces a useful, concrete and tangible result, based on the factors discussed below. Applicant submits that the claimed invention transforms an article or physical object to a different state or thing, or alternatively, produces a useful, concrete, and tangible result.

a) Physical transformation:

Claim 1-32 recite, among other things, (1) providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters, the first peer and second peer being communicated over a network; (2) performing a first exponentiation operation to generate a first public key from the second peer using at least one parameter of the plurality of first parameters and a first private key from the second peer, wherein the first parameters being digital signature standard parameters; (3) providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters; (4) performing a second exponentiation operation to generate a first shared secret key for the second peer using at least one parameter from the plurality of first parameters; and (5) performing a third exponentiation operation to generate a second shared secret key for the first peer using the first public key from the second peer and a private key from the first peer.

A (first, second) certificate, a (first, second) peer, a (first private, first public, shared secret) key, a network, and a plurality of (first, second) parameters, are all

physical entities. All of these are physical objects, not abstract ideas like democracy, freedom, or capitalism.

Providing a first certificate from a first peer to a second peer is a transformation that transfers the first certificate from a first peer to a second peer. Performing a first exponentiation operation is a transformation that computes the exponentiation from a parameter and a first private key to generate a first public key. Providing a second certificate and the first public key from the second peer to the first peer is a transformation to move or transfer the second certificate and the first public key from the second peer to the first peer. Performing a second exponentiation operation is a transformation that computes the exponentiation from at least one parameter from the plurality of first parameters to generate a first shared secret key. Performing a third exponentiation operation is a transformation that computes the exponentiation from the first public key and a private key to generate a second shared secret key for the first peer.

Since all five operations (providing a first certificate, performing a first exponentiation operation, providing a second certificate, performing a second exponentiation operation, performing a third exponentiation operation) represent physical transformations of physical entities (certificate, peer, key, network, parameters) or reduction of the parameters to a different state or thing, the claimed invention satisfies the physical transformation requirement. Thus, the claimed invention is statutory.

b) Useful, concrete, and tangible result:

In determining whether the claim is for a "practical application," the focus is not on whether the steps taken to achieve a particular result are useful, tangible and concrete, but rather that the final result achieved by the claimed invention is "useful, tangible and concrete." (Guidelines, page 20). Here, the final result of the claimed invention is the shared secret key for the first peer. The performed action is useful, tangible, and concrete.

Useful: For an invention to be "useful" it must satisfy the utility requirement of section 101. The USPTO's official interpretation of the utility requirement provides that the utility of an invention has to be (i) specific, (ii) substantial and (iii) credible. MPEP §2107 and Fisher, 421 F.3d, 76 USPQ2d at 1230. Here, the utility of the claimed invention is specific, substantial, and credible. It is specific because it aims at a specific task of generating a shared secret key for a first peer in a computing device. It is substantial because it solves a significant problem in key exchange based on certificates. It is credible because it provides a novel technique using methods that may be verified or confirmed by persons skilled in the art, such as providing the certificate and performing an exponentiation operation.

Tangible: The tangible requirement does require that the claim must recite more than a §101 judicial exception, in that the process claim must set forth a practical application of that §101 judicial exception to produce a real-world result. In other words, the opposite meaning of "tangible" is "abstract." Here, the claimed invention produces a real-world result because the performed actions results in a shared secret key for a peer, a computing device. It does not represent an abstract idea such as democracy, freedom, or capitalism.

Concrete: The "concrete" requirement means that the process must have a result that can be substantially repeatable or the process must substantially produce the same result again. The opposite of "concrete" is unrepeatable or unpredictable. Here, the claimed invention is substantially repeatable and predictable. As long as there are parameters and a first private key from the second peer, the claimed invention would produce the same result again.

In summary, the claimed invention satisfies all the statutory requirements under 35 U.S.C. §101 as provided by the Guidelines. Therefore, Applicant respectfully requests the rejection under § 101 be withdrawn.

II. REJECTIONS UNDER 35 U.S.C. § 103

The Examiner rejected: 1) claims 1-32 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,792,530 issued to Qu et al. ("Qu"), and in view of U.S. Patent No. 7,076,061 issued to Lenstra et al. ("Lenstra"); 2) claims 33-35 under 35 U.S.C. §103(a) as being unpatentable over Qu et al., and Lenstra et al., and further in view of U.S. Patent No. 7,222,187 issued to Yeager et al. ("Yeager").

Applicant respectfully traverses the rejections for the following reasons. Qu discloses a method of generating an identity-based public key in a secure digital communication system, having at least one trusted entity CA and subscribers entities (Col. 2, lines 26-36). Qu discloses the steps of (a) for each entity A, the CA selecting a unique identity I_A distinguishing the entity A; (b) generating a public key reconstruction public data γ_A of entity A by mathematically combining a generator of the trusted party CA with a private value of the entity A, such that the pair (I_A, γ_A) serves as A's implicit certificates; and combining the implicit certificate information (I_A, γ_A) in accordance with a mathematical function $F(I_A, \gamma_A)$ to derive an entity information f (Col. 2, lines 38-47). The certificate scheme can be used with any scheme, which is required to verify the certificate. This may be demonstrated by referring to the DSA ... (Col. 3, lines 57-67). Qu discloses an ID-based certificate generation process, which is not the same as the claimed invention. In the present invention, it is assumed that DSA type certificate has already been generated and distributed among the first and second peers by CA. Unlike Qu, the claimed invention uses certificate parameters for a key exchange. Furthermore, the claim invention is not a certificate public key generation process as is in Qu (Col. 2, lines 25-60. More importantly, Qu discloses a key exchange process that requires 4 exponentiation operations (2 on Alice side and 2 on Bob side), when the claimed invention requires only 3 exponentiation operations.

Qu discloses that CA chooses random integer $1<C_A<q$, then computes A's public key reconstruction public data, which serves as A's implicit certificate. However, unlike the present invention, Qu does not disclose the use of Y_R as a key exchange public key. Qu discloses an algorithm for generating special public key, which becomes a part of generated certificate. The present invention, on the other hand, does not generate public key for certificates. The public key (Y_R) in the claimed invention is used for key exchange only. It does not store in certificate (Col. 9, lines 20-67). Furthermore, in contrast to the claimed invention, in Qu, these operations are done by CA and resulting data are not change for certificate life time when in the claimed invention, these operations are done by peers and they change during each new key exchange time. Furthermore, in the claimed invention, after second exponential operation, first peer generates shared secret key Y_{ssk} using second peer public key, when in Qu, the second exponentiation operation (Col. 17, lines 1-21) is done by CA2. It is not done using CA1 public key.

Qu discloses that in its phase 2, CA3 applies for implicit certified public key from CA2 (Col. 17, lines 25-45) and in phase 3, a user A applies for implicit certified public keys from CA3 (Col. 17, lines 64-67). Qu further discloses that peer Alice computes the shared key K_A (where $K_A = (\alpha^{ay})^{xa-1} = \alpha^{xy}$) and peer Bob computes the shared key K_B (where $K_B = (\alpha^{bx})^{yb-1} = \alpha^{xy}$... (Col. 20, lines 1-8). Qu discloses MTI/C0 key exchange protocol that peer Alice chooses an integer x and computes some number using peer Bob's ID based public key and they peer Alice sends it to peer Bob. The same kind of operation is done by peer Bob. In Qu, key exchange protocol is used both certificate public keys. In the claimed invention, first peer (i.e. Alice) chooses integer x and does the first exponentiation operation then result is sent to second peer (i.e., Bob). The first peer's second exponential operation only uses second peer's certificate public key. Second peer does not use first peer's public key. It uses the result of first exponentiation operation. Both peers in Qu perform the same operations on both sides (two operations each

sides) (Col. 17, lines 25-45, lines 64-47 and Col. 20, lines 1-8). The number of operations performed in Qu is 4, when in the present invention, only 3 operations are performed.

The Examiner contends that Qu teaches reconstructing user A's public key that needs only 3 known basis exponentiation operations and 3 multiplication operations. When the signature is valid, CA2, CA3, and user A's public key are implicitly verified (Col. 18, lines 22-28). This is nothing more than the using of an ID-based public key for signature verification process, which requires 3 exponentiation and 3 multiplication operations. In other words, what disclosed in Qu is not the same as the claimed invention since the claimed invention is about using key exchange algorithm based on DSA type certificate. The claimed invention is not about signature generation/verification mechanisms.

Lenstra discloses key generation and cryptographic applications in public key cryptography, by both reducing: (1) the bit-length of public keys and other messages ..., and (2) the computation effort required to generate keys, to encrypt/decrypted and the generate/verify digital signatures (Col. 2, lines 20-27). Lestra's XTR (abbreviation for Efficient and Compact Subgroup Trace Representation) public key system is a representation of elements, and 2.4.4 key generation algorithms are not related to propose key exchange algorithm (Col. 2, lines 20-27). While Lenstra discloses providing key generation improvement in the above-mentioned cryptosystem, the present invention works on GF(p) field and it is applied only for key exchange. The claimed invention is based on DSA type of certificate parameters p, q, g only. Lenstra further discloses XTR-CSC (Cramer-Shoup Crytosystem) ....

Yeager discloses that in order to interact with the peers, the peer needs to be connected to some kind of network, such as IP, Bluetooth, or Havi, among others (Col 27, lines 29-35). Yeager further discloses that peer-to-peer platform may be independent of transport protocols. For example, the peer-to-peer platform may be implemented on top of TCP/IP, HTTP, Bluetooth, Home-PNA,

and other protocols (Col. 33, lines 21-25). Yeager, however, does not disclose generating a secret key by 3 exponentiation operations DSA parameters.

Qu, Lenstra, and Yeager, taken alone or in any combination, do not disclose, suggest, or render obvious generating a secret key by 3 exponentiation operations DSA parameters. This aspect of the invention is supported in the specification in paragraphs 7-8, 39-43, and is recited in independent claims 1, 9, 17, and 25.

Therefore, Applicant believes that independent claims 1, 9, 17, 25 and their respective dependent claims are distinguishable over the cited prior art references. Accordingly, Applicant respectfully requests the rejections under 35 U.S.C. § 103(a) be withdrawn.

CONCLUSION

In view of the amendments and remarks made above, it is respectfully submitted that the pending claims are in condition for allowance, and such action is respectfully solicited. If it is believed that a telephone conversation would expedite the prosecution of the present application, or clarify matters with regard to its allowance, the Examiner is invited to contact the undersigned attorney at the number listed below.

The Commissioner is hereby authorized to charge payment of any required fees associated with this Communication or credit any overpayment to Deposit Account No. 04-1175.

Respectfully submitted,

PIONEER NORTH AMERICA, INC.

Dated: 06/18/08

Caroline T. Do, Esq.
Reg. No. 47,529

PIONEER NORTH AMERICA, INC.
INTELLECTUAL PROPERTY DEPARTMENT
2265 E. 220th Street
Long Beach, CA 90810
(310) 952-3300

P:\ABG\PPD\PR\1803\01\AMEND_04.DOC